Stellen Sie Reveal (x) Ultra in AWS bereit

Veröffentlicht: 2024-01-22

In diesem Handbuch erfahren Sie, wie Sie den ExtraHop Reveal (x) Ultra-Sensor über den AWS Marketplace bereitstellen.

Nachdem Sie den Sensor bereitgestellt haben, konfigurieren Sie Spiegelung des AWS-Datenverkehrs oder RPCAP (RPCAP), um den Verkehr von Remote-Geräten an den Sensor weiterzuleiten.

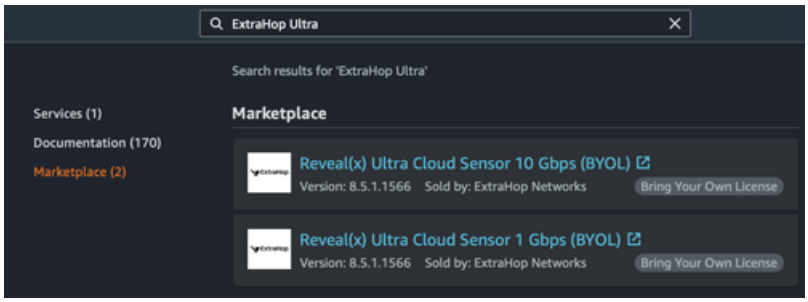
Anforderungen an das System

Stellen Sie sicher, dass Sie über alles verfügen, was Sie für die erfolgreiche Bereitstellung des benötigen Sensor:

- Ein AWS-Konto
- Eine ExtraHop Reveal (x) Ultra-Lizenz oder ein Produktschlüssel
- Eine VPC, in der die Sensor wird eingesetzt
- Zwei ENI-Subnetze. Ein Subnetz für den Zugriff auf die Verwaltungsschnittstelle des Sensor und ein Subnetz, das den Verkehr an den Sensor weiterleitet. Beide Subnetze müssen sich in derselben Availability Zone befinden.

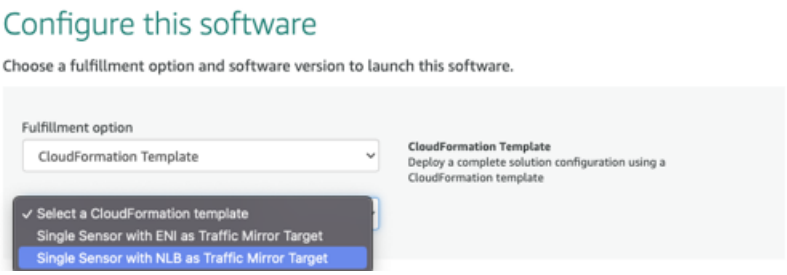
Setzen Sie den Sensor ein

1. Melden Sie sich bei Ihrer AWS-Managementkonsole an.
2. Suchen Sie im Marketplace nach ExtraHop Ultra Sensoren.

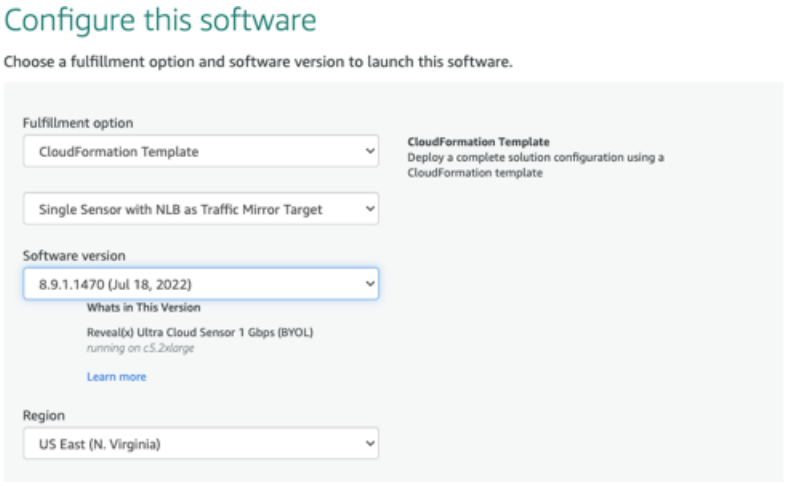


3. Klicken Sie auf eine der folgenden Optionen Sensor Namen:
   - **Reveal (x) Ultra-Cloud-Sensor 1 Gbit/s (BYOL)**
   - **Reveal (x) Ultra-Cloud-Sensor 10 Gbit/s (BYOL)**
4. klicken **Weiter abonnieren**.
5. Lesen Sie die Allgemeinen Geschäftsbedingungen von ExtraHop und klicken Sie dann auf **Bedingungen akzeptieren**.
6. Nachdem der Abonnementvorgang abgeschlossen ist, klicken Sie auf **Weiter zur Konfiguration**.
7. Wählen **CloudFormation-Vorlage** von der **Erfüllungsoption** Drop-down-Liste.

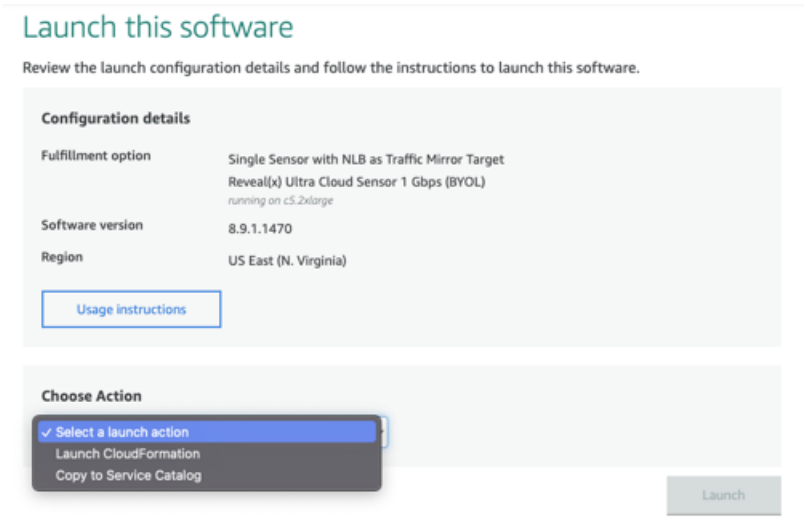
8. Wählen Sie eine der folgenden CloudFormation-Vorlagen aus der Drop-down-Liste aus:
   - **Einzelsensor mit ENI als Verkehrsspiegelziel**
   - **Einzelsensor mit NLB als Verkehrsspiegelziel**. Diese Option wird empfohlen, wenn Sie mehr als zehn Verkehrsquellen haben.



9. Wählen Sie eine Firmware-Version aus der **Version der Software** Drop-down-Liste.
10. Wählen Sie Ihre AWS-Region aus der **Region** Drop-down-Liste.



11. klicken **Weiter zum Start**.
12. Wählen Sie auf der Seite Diese Software starten unter Aktion auswählen **Starten Sie CloudFormation**.



13. klicken **Starten**.
14. Lassen Sie auf der Seite Stack erstellen die Standardeinstellungen unverändert und klicken Sie auf **Weiter**.
15. Geben Sie auf der Seite „Stack-Details angeben“ einen Namen in das **Name des Stapels** Feld zur Identifizierung Ihrer Instanz in AWS.
16. Konfigurieren Sie im Abschnitt Netzwerkkonfiguration die folgenden Felder:

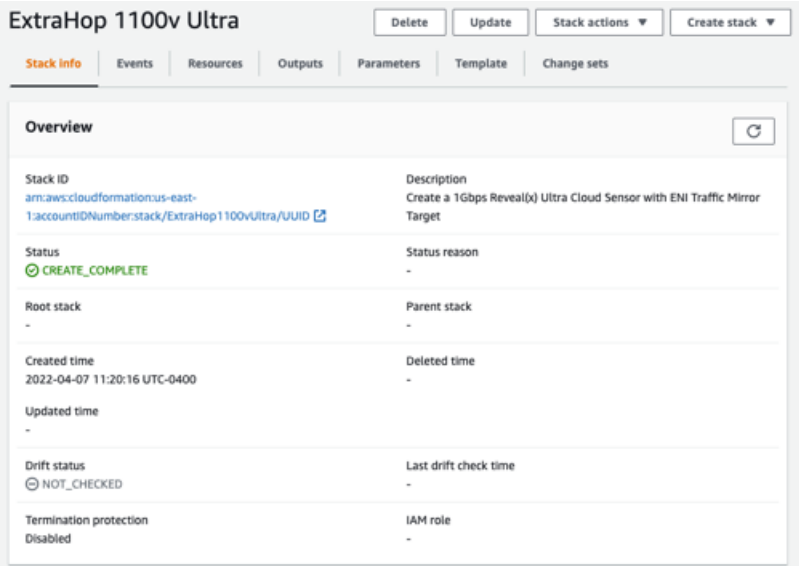
    • **VPCID:** Wählen Sie die VPC aus, in der der Sensor eingesetzt werden soll

    • **MGMT-Subnetz-ID:** Wählen Sie das Subnetz aus, in dem die Management-ENI bereitgestellt werden soll

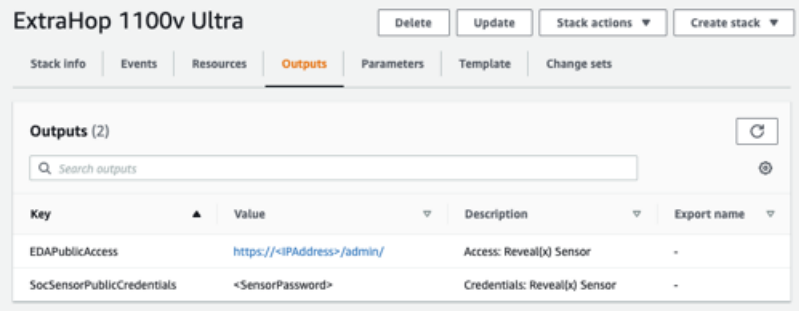
    • **Subnetz-ID erfassen:** Wählen Sie das Subnetz aus, in dem die Datenerfassungs-ENI bereitgestellt werden soll

    • **Fernzugriff CIDR:** Geben Sie einen CIDR-IP-Bereich ein, um den Benutzerzugriff auf die Instanz einzuschränken. Wir empfehlen Ihnen, einen vertrauenswürdigen IP-Adressbereich zu konfigurieren.
17. Wählen Sie im Abschnitt ExtraHop-Konfiguration eine der folgenden Optionen für das Feld publicIP aus:

    - Wählen **falsch** wenn Sie keine öffentlich zugängliche IP-Adresse wünschen.
    - Wählen **wahr** wenn Sie möchten, dass der Sensor Benutzern über das öffentliche Internet zur Verfügung steht. Die `MgmtSubnetID` Das im vorherigen Schritt angegebene Subnetz muss ein öffentliches Subnetz sein.
18. Optional: Geben Sie im Abschnitt Andere Parameter eine AMI-ID für die Quell-Instance ein.
19. **Klicken Sie auf Weiter**.
20. Fügen Sie im Abschnitt Tags ein oder mehrere Tags hinzu und klicken Sie dann auf **Weiter**.
21. Überprüfen Sie Ihre Konfigurationseinstellungen und klicken Sie dann auf **Stapel erstellen**.
22. Warten Sie, bis die Erstellung abgeschlossen ist. Die `CREATE_COMPLETE` Der Status wird auf der Stack-Infoseite angezeigt, wenn die Stack-Erstellung erfolgreich war.



23. Klicken Sie auf **Ausgänge** Registerkarte.



24. Kopiere das **Öffentliche Zugangsdaten für SOC Sensor** Wert. Dies ist das Setup-Benutzerpasswort, das für die Anmeldung am ExtraHop-System erforderlich ist.
25. Klicken Sie auf **Öffentlicher Zugang zu EDA** Wert-URL, um zur Seite mit den Administrationseinstellungen des Sensor zu gelangen.

Nächste Schritte

- Registrieren Sie Ihr ExtraHop-System
- Konfigurieren Sie den Sensor Netzwerkschnittstellen durch Anklicken **Konnektivität** in den Administrationseinstellungen. Stellen Sie sicher, dass **Verwaltung** ist auf Interface 1 ausgewählt. Wählen Sie für Interface 2 eine der folgenden Optionen:
  - Für die 1 Gbit/s Sensor, wählen **Geschäftsleitung + RPCAP/ERSPAN/VXLAN/GENEVE Target**.
  - Für die 10 Gbit/s Sensor, wählen **Leistungsstarkes ERSPAN/VXLAN/GENEVE-Target**.

  Wichtig: Um die beste Leistung bei der ersten Gerätesynchronisierung zu gewährleisten, schließen Sie alle Sensoren an die Konsole an und konfigurieren Sie dann die Weiterleitung des Netzwerkverkehrs zu den Sensoren.
- (Empfohlen) konfigurieren Spiegelung des AWS-Datenverkehrs oder RPCAP (RPCAP), um den Verkehr von Remote-Geräten an den Sensor weiterzuleiten.
- (Fakultativ) Weiterleiten von geneve-gekapseltem Datenverkehr von einem AWS Gateway Load Balancer.
- Führen Sie die empfohlenen Verfahren in der Checkliste für die Zeit nach der Bereitstellung.

Erstellen Sie ein Verkehrsspiegelziel

Führen Sie diese Schritte für jede ENI aus, die Sie erstellt haben.

1. Kehren Sie zur AWS-Managementkonsole zurück.
2. Klicken Sie im oberen Menü auf **Dienstleistungen**.
3. Klicken Sie im Abschnitt Networking & Content Delivery auf **VPC**.
4. Klicken Sie im linken Bereich unter Traffic Mirroring auf **Spiegelziele**.
5. Klicken **Verkehrsspiegelziel erstellen** und füllen Sie die folgenden Felder aus:

Option	Beschreibung
Namensschild	(Optional) Geben Sie einen beschreibenden Namen für das Ziel ein.
Beschreibung	(Optional) Geben Sie eine Beschreibung für das Ziel ein.
Typ des Ziels	Wählen **Netzwerk-Schnittstelle**.
Ziel	Wählen Sie die ENI aus, die Sie zuvor erstellt haben.

6. Klicken **Erstellen**.

Notieren Sie sich die Ziel-ID für jede ENI. Sie benötigen die ID, wenn Sie eine Traffic Mirror-Sitzung erstellen.

Erstellen Sie einen Verkehrsspiegelfilter

Sie müssen einen Filter erstellen, um den Datenverkehr von Ihren ENI Traffic Mirror-Quellen zu Ihrem ExtraHop-System zuzulassen oder einzuschränken. Wir empfehlen die folgenden Filterregeln, um zu verhindern , dass doppelte Frames von Peer-EC2-Instances, die sich in einer einzelnen VPC befinden, auf die Sensor.

- Der gesamte ausgehender Datenverkehr wird gespiegelt auf Sensor, ob der Datenverkehr von einem Peer-Gerät an ein anderes im Subnetz gesendet wird oder ob der Datenverkehr an ein Gerät außerhalb des Subnetzes gesendet wird.
- Eingehender Verkehr wird nur gespiegelt auf Sensor wenn der Datenverkehr von einem externen Gerät stammt. Diese Regel stellt beispielsweise sicher, dass eine App-Serveranfrage nicht zweimal gespiegelt wird: einmal vom sendenden App-Server und einmal von der Datenbank , die die Anfrage empfangen hat.
- Regelnummern bestimmen die Reihenfolge, in der die Filter angewendet werden. Regeln mit niedrigeren Zahlen, z. B. 100, werden zuerst angewendet.

> **Wichtig:** Diese Filter sollten nur angewendet werden, wenn alle Instanzen in einem CIDR-Block gespiegelt werden.

1. Klicken Sie in der AWS-Managementkonsole im linken Bereich unter Traffic Mirroring auf **Spiegelfilter**.
2. klicken **Verkehrsspiegelfilter erstellen** und füllen Sie die folgenden Felder aus:

Option	Beschreibung
Namensschild	Geben Sie einen Namen für den Filter ein.
Beschreibung	Geben Sie eine Beschreibung für den Filter ein.
Netzwerkdienste	Wählen Sie den **Amazon-DNS** Checkbox.

3. In der Regeln für eingehenden Datenverkehr Abschnitt, klicken **Regel hinzufügen** und füllen Sie dann die folgenden Felder aus:

Option	Beschreibung
Zahl	Geben Sie eine Zahl für die Regel ein, z. B. `100`.

Option	Beschreibung
Regelaktion	Wählen **ablehnen** aus der Dropdownliste.
Protokoll	Wählen **Alle Protokolle** aus der Dropdownliste.
CIDR-Quellblock	Geben Sie den CIDR-Block für das Subnetz ein.
CIDR-Zielblock	Geben Sie den CIDR-Block für das Subnetz ein.
Beschreibung	(Optional) Geben Sie eine Beschreibung für die Regel ein.

4. In der Regeln für eingehenden Datenverkehr Abschnitt, klicken **Regel hinzufügen** noch einmal und füllen Sie dann die folgenden Felder aus:

Option	Beschreibung
Zahl	Geben Sie eine Zahl für die Regel ein, z. B. `200`.
Regelaktion	Wählen **akzeptieren** aus der Dropdownliste.
Protokoll	Wählen **Alle Protokolle** aus der Dropdownliste.
CIDR-Quellblock	Typ `0.0.0.0/0`.
CIDR-Zielblock	Typ `0.0.0.0/0`.
Beschreibung	(Optional) Geben Sie eine Beschreibung für die Regel ein.

5. In der Regeln für ausgehenden Datenverkehr Abschnitt, klicken **Regel hinzufügen** und füllen Sie dann die folgenden Felder aus:

Option	Beschreibung
Zahl	Geben Sie eine Zahl für die Regel ein, z. B. `100`.
Regelaktion	Wählen **akzeptieren** aus der Dropdownliste.
Protokoll	Wählen **Alle Protokolle** aus der Dropdownliste.
CIDR-Quellblock:	Typ `0.0.0.0/0`.
CIDR-Zielblock:	Typ `0.0.0.0/0`.
Beschreibung	(Optional) Geben Sie eine Beschreibung für die Regel ein.

6. klicken **Erstellen**.

Erstellen Sie eine Traffic Mirror-Sitzung

Sie müssen für jede AWS-Ressource, die Sie überwachen möchten, eine Sitzung erstellen. Sie können maximal 500 Traffic Mirror-Sitzungen pro erstellen Sensor.

Wichtig: Um zu verhindern, dass Spiegelpakete gekürzt werden, legen Sie den MTU-Wert der Traffic Mirror-Quellschnittstelle auf 54 Byte unter dem MTU-Zielwert des Traffic Mirrors für IPv4 und 74 Byte unter dem MTU-Zielwert des Traffic Mirrors für IPv6 fest. Weitere Informationen zur Konfiguration des Netzwerk-MTU-Werts finden Sie in der folgenden AWS-Dokumentation: Network Maximum Transmission Unit (MTU) für Ihre EC2-Instance.

1. Klicken Sie in der AWS-Managementkonsole im linken Bereich unter Traffic Mirroring auf **Spiegelsitzung**.
2. Klicken **Traffic Mirror-Sitzung erstellen** und füllen Sie die folgenden Felder aus:

Option	Beschreibung
Namensschild	(Optional) Geben Sie einen beschreibenden Namen für die Sitzung ein.

Option	Beschreibung
Beschreibung	(Optional) Geben Sie eine Beschreibung für die Sitzung ein
Spiegelquelle	Wählen Sie die Quelle ENI aus. Die Quell-ENI ist normalerweise an die EC2-Instance angehängt , die Sie überwachen möchten.
Spiegelziel	Wählen Sie die Traffic Mirror-Ziel-ID aus, die für die Ziel-ENI generiert wurde.
Nummer der Sitzung	Typ `1`.
VNI	Lassen Sie dieses Feld leer.
Länge des Pakets	Lassen Sie dieses Feld leer.
Filtern	Wählen Sie im Dropdownmenü die ID für den Traffic Mirror-Filter aus, den Sie erstellt haben.

3. Klicken **Erstellen**.